BRYAN SCHRODER
Acting United States Attorney

RICHARD L. POMEROY
YVONNE LAMOUREUX
ADAM ALEXANDER
Assistant U.S. Attorneys
Federal Building & U.S. Courthouse
222 West Seventh Avenue, #9, Rm. 253
Anchorage, Alaska 99513-7567
Telephone: (907) 271-5071
Facsimile: (907) 271-2344
Richard.Pomeroy@usdoj.gov
Yvonne.Lamoureux@usdoj.gov
Adam.Alexander@usdoj.gov

ETHAN ARENSON
HAROLD CHUN
FRANK LIN
Trial Attorneys
Computer Crime & Intellectual Property Section
1301 New York Avenue, NW, Suite 600
Washington, DC 20005
Telephone: (202) 514-1026
Facsimile: (202) 514-6113
Ethan.Arenson@usdoj.gov
Harold.Chun@usdoj.gov
Frank.Lin@usdoj.gov

Attorneys for Plaintiff United States

//

//

//

//

//

//

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Case No. 3:17-cv-_____
	)	
v.	)	**FILED *EX PARTE***
	)	**AND UNDER SEAL**
PETER YURYEVICH LEVASHOV,	)	
a.k.a. "Petr Levashov," "Peter Severa,"	)	
"Petr Severa," and "Sergey Astakhov",	)	
	)	
Defendant.	)	

UNITED STATES' MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff, the United States of America, by and through its attorneys, Bryan Schroder, Acting United States Attorney for the District of Alaska, Kenneth A. Blanco, Acting Assistant Attorney General, Richard L. Pomeroy, Yvonne Lamoureux, and Adam Alexander, Assistant United States Attorneys, and Ethan Arenson, Harold Chun and Frank Lin, Trial Attorneys, pursuant to 18 U.S.C. §§ 1345, 2521, and Federal Rule of Civil Procedure 65, hereby seeks an *ex parte* temporary restraining order commanding the Defendant to halt a decade-long fraud and wiretapping scheme that is harming individuals and businesses in the United States and around the world.

I. OVERVIEW

The defendant in this case is one of the world's most notorious criminal spammers, who for more than ten years has been engaged in the distribution of unsolicited, fraudulent, and malicious emails. The engine powering the Defendant's spam operation is the Kelihos botnet – a network of victim computers deliberately infected with malicious software and controlled by the Defendant. Without the knowledge or consent of the owners of the infected computers, the Defendant uses this network to send massive quantities of spam primarily targeting individuals in the United States. The Defendant makes further use of the victim computers by illegally intercepting network traffic transiting the computers in order to steal user credentials and by installing other forms of malicious software ("malware").

The Defendant's long criminal career has not escaped the attention of U.S. law enforcement. More than a decade ago, the Defendant was indicted in the Eastern District of Michigan for email and wire fraud. The charges arose out of the Defendant's use of illegal spam to promote pump-and-dump penny stock schemes.

In 2009, the Defendant was again the subject of criminal charges, this time in the District of Columbia. The D.C. criminal complaint, which was dismissed because the Defendant could not be located, charged the Defendant with computer fraud violations arising from his operation of the "Storm" botnet, a predecessor to Kelihos that was also used to distribute illegal spam.

The Defendant's continued criminal activity, including his operation of the Kelihos botnet, led both the District of Alaska and the District of Connecticut to open investigations of the Defendant. In late March 2017, the FBI learned that the Defendant had left his home in Russia and was planning to stay for several weeks in Spain. [redacted] Accordingly, in this action, the United States seeks injunctive relief commanding the Defendant to stop using the Kelihos botnet to defraud and wiretap American citizens and businesses. To give effect to this prohibition, the United States seeks permission to employ a series of technical measures designed to disrupt the Defendant's malware and attempt to liberate infected computers. Specifically, the United States seeks an Order: (1) authorizing the use of the technical measures specified below to disrupt the Defendant's control of the botnet; and (2) directing two U.S. Internet Domain Registries to redirect connection requests made to domain names used to control the botnet to substitute servers established by order of this Court.

---

[1] [redacted]

In addition to the civil relief sought above, the Government has also applied for a Pen Register/Trap and Trace Order that would authorize the collection of the dialing, routing, addressing, and signaling information of communications sent by the Kelihos malware to the substitute servers and other infrastructure established pursuant to the TRO sought by the Government. This information would be disseminated to internet service providers and other assisting entities that would notify Kelihos victims and provide instruction on how to remove these infections from their computers.

Finally, in an abundance of caution, the Government seeks a search warrant to authorize the technical measures described in this memorandum in the event any of them are deemed a search or seizure of a victim's computer.

This action is the latest in a string of cases brought by public and private sector entities to combat malicious software, and is very similar to the successful Dridex, Gameover Zeus and Coreflood botnet disruptions, which were initiated in the Western District of Pennsylvania and the District of Connecticut. *See United States v. Ghinkul*, No. 2:2015-CV-1315 (W.D. Pa., filed October 8, 2015) ("Dridex"); *United States v. Bogachev*, No. 2:14-CV-0685 (W.D. Pa., filed May 26, 2014) ("Gameover Zeus"), *United States v. John Doe 1 et al.* No. 3:11-CV-00561 (D. Conn., filed Apr. 11, 2011) ("Coreflood"). Coreflood, Gameover Zeus, and Dridex, like Kelihos, were botnets used by criminals to intercept credentials transmitted by victim computers. To disable these botnets, the United States used the same

authorities invoked here to deny the botnet operators access to the infrastructure necessary to control the botnet. In each of these cases, the Government also received judicial authorization to establish a substitute server to replace the command and control infrastructure controlled by the botnet operators. In each of these cases, the government's actions successfully crippled the botnet.

The Defendant is causing significant harm in this District, in the United States, and around the world. To disrupt his criminal activity and prevent the Kelihos botnet from falling into the hands of another criminal, the United States respectfully requests that this Court enter the proposed temporary restraining order ("TRO") and order the Defendant to show cause why a preliminary injunction should not be granted.

II. BACKGROUND ON KELIHOS

The total number of computers infected with Kelihos at any one time can vary. *See* Declaration of Special Agent Elliott Peterson, attached hereto ("Peterson Declaration") at ¶8. At times, over 100,000 computers have been simultaneously infected worldwide with Kelihos. *Id.* Presently, the number sits between 25,000 and 100,000, with roughly 5-10% of victims located in the United States. *Id.* Kelihos is very difficult for computer users to detect, as it is designed to persist on a victim's computer despite any overt actions by the victim to remove it. *Id.*

Kelihos's principal functions are to (1) distribute high volumes of spam email to further criminal schemes; (2) install malicious payloads, such as ransomware;

and (3) harvest user credentials from infected computers. *Id.* ¶ 11. These schemes commonly target the United States and other English speaking nations. *Id.* ¶ 24.

A. Kelihos's Spam Distribution

Kelihos distributes spam in several ways. First, Kelihos can distribute spam from infected computers directly. *Id.* ¶ 17. Kelihos can command infected computers to function as covert mail servers and distribute spam to recipient email addresses passed to the computer from the botnet without alerting the owner. *Id.* In these cases, Kelihos generates "sender" email addresses that are randomly generated first and last name combinations not obviously associated with the true account from which the spam came. *Id.* Known as "spoofing" the result is that the spam will be made to appear to come from [username]@gmail.com when in reality it was sent by an infected computer with no association to the referenced email account. *Id.* Spoofing makes the spam much more difficult to detect and block, while also concealing the true origins of the email messages. *Id.*

The Kelihos botnet can also send spam directly from mail servers, such as those owned by Earthlink or 1&1 Mail & Media, by gaining unauthorized access to them through the use of authentic user credentials harvested by Kelihos. *Id.* In those instances, the spam is, in essence, sent from the victim's email address through the mail server, but without the victim's knowledge or authorization. *Id.*

It is through use of the two aforementioned techniques that Kelihos sustains such a high volume of spam distribution. *Id.* ¶ 18. Kelihos is believed to be

responsible for the distribution of hundreds of millions of spam messages within a calendar year, and is capable of distributing thousands of messages within a matter of minutes. *Id.*

The types of spam emails the Defendant uses Kelihos to generate varies based on the needs of his customer base, but investigators have observed Kelihos being used for the following purposes:

- Kelihos generates massive volumes of spam emails directing recipients to illicit web sites advertising the sale of branded pharmaceuticals at below market rates and without the need for a prescription, indicating that the drugs offered are likely counterfeit. *Id.* ¶ 13.
- Kelihos distributes high volumes of emails to effectuate penny stock "pump-and-dump" schemes intended to manipulate the price of thinly-traded securities. *Id.* ¶ 14. In these messages, the recipient is led to believe that a specific stock will soon trade at a much higher value. *Id.* Because these emails target stocks which generally experience very low trading volume, they are vulnerable to price manipulation associated with small increases in trade volume. *Id.*
- Kelihos is also a primary vector for fraudulent affiliate recruitment scams commonly called "work from home." *Id.* ¶ 15. In these messages, the unwitting recipient is directed to an email address or website from which they can receive more information about

performing escrow or "private buyer" services. *Id.* These schemes are primarily vehicles to further money laundering enterprises. *Id.* For example, in an escrow scheme, individuals are instructed to receive and transfer funds in short time periods, often 1-3 days. *Id.* The incoming funds are usually proceeds of other criminal schemes which are then laundered through the unwitting recipient's bank account. *Id.* Due to the short time period from which money is received and then resent, the victim often is left responsible for the full amount laundered through their accounts after the financial institution detects the fraud and ceases further payment. *Id.*

- Kelihos is also employed to distribute malicious software via URL hyperlinks contained within email messages. *Id.* ¶ 18. Unwitting users are encouraged by the contents of the email to click on a hyperlink, which leads them to a web location that then attempts to install malicious software. *Id.*

B. Kelihos Issues Malicious Commands

Kelihos can also command infected computers to download and execute malware directly. *Id.* ¶ 19. By commanding Kelihos-infected computers to download and execute malicious files – including ransomware and banking trojans, – the Defendant enables extortion, the theft of victim's financial credentials, and permits criminals to take near total control of victims' computers. *Id.* These

programs are typically installed by the Defendant on behalf of other criminals, who pay the Defendant for each successful installation. *Id.* This allows the Defendant to further monetize his botnet beyond the distribution of spam. *Id.*

C. Kelihos Harvests User Credentials

In addition to distributing spam email and malicious payloads, the Kelihos malware also harvests user credentials from victim computers through a number of methods. *Id.* ¶ 20. First, Kelihos searches text-based files stored on victim computers for email addresses. *Id.* Second, Kelihos searches locations on victim computers for files known to contain usernames and passwords, including files associated with Internet browsers Chrome, Firefox, and Internet Explorer. *Id.* Any email addresses and passwords located in these searches are harvested by Kelihos and subsequently transmitted back to the Defendant. *Id.*

To capture additional user credentials, Kelihos installs a software program called WinPCAP on infected machines. *Id.* ¶ 21. WinPCAP is a powerful packet capture utility that intercepts, in real time, electronic communications traversing the victim computer's network card. *Id.* Usernames and passwords found within this network traffic are transmitted back to the Defendant. *Id.*

III. THE DEFENDANT

A multi-year investigation by the Federal Bureau of Investigation (FBI) has revealed that Defendant, a citizen and resident of Russia, operates the Kelihos Botnet. *Id.* ¶¶ 4, 41. As indicated above, Defendant is not a new face to law

enforcement, as he has previously been charged twice before: (1) indicted once in the Eastern District of Michigan for conspiracy to commit mail, electronic mail and wire fraud in violation of 18 U.S.C. §§ 371, 1037(a)(2)-(a)(3), 1037(b)(2)(C), 1341, and 1343 and several substantive counts of violating 18 U.S.C. §§ 1037(a)(2), 1037(b)(2)(C), and Section 2, arising from his involvement in distributing spam to further a pump and dump stock scheme; and (2) charged in a criminal complaint filed in the U.S. District Court for the District of Columbia, which in 2009 charged LEVASHOV in his true name with two substantive counts of violating 18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(a)(5)(A)(i) and 1030(a)(5)(B)(V), as well as one count of conspiracy to commit these offenses in violation of 18 U.S.C. § 371, arising from operating a botnet known as the Storm Botnet. *Id.* ¶¶ 5-6. The complaint in the District of Columbia was dismissed in 2014 because the Defendant could not be located and arrested. *Id.* ¶ 6. The Defendant's long and prolific career as a criminal spammer has earned him the sixth spot in the anti-spam organization Spamhaus's World's Ten Worst Spammers list. *Id.* ¶ 7.[2]

Defendant has been connected by the FBI to the operation of Kelihos through numerous ways. First, the FBI identified an overseas server, bearing IP address 94.242.250.88, that was used to facilitate the Kelihos botnet. *Id.* ¶ 42. Monitoring of the server showed that it was utilized on thousands of occasions to log into email

---

[2] *See* https://www.spamhaus.org/statistics/spammers/, last observed on March 29, 2017.

account pete777@mail.ru. *Id.* ¶ 48. An Internet search of pete777@mail.ru revealed that the website 3038.org/listn.html associated the email address with Pete LEVASHOV, a web programmer located in Russia. *Id.* Moreover, the 3038.org website appeared to be for a high school located in St. Petersburg, Russia, the hometown of Defendant. *Id.* Business records obtained from Apple confirm that pete777@mail.ru is associated with Petr LEVASHOV, who resides in Russia. *Id.* ¶ 49. Moreover, Apple records indicate that the relevant iCloud account was registered from the IP address 83.243.67.25 and had a secondary email account levashov@knyazev-spb.ru. *Id.* Records also indicate its Apple Digital Signaling Identifier (DSID) as 1972828024. *Id.*

Records from Google indicate that the IP address 83.243.67.25 was utilized to register the Google account peteknyazev777@gmail.com. *Id.* ¶ 50. The common configuration of "pete", "knyazev" and "777" are noteworthy. Moreover, Google records indicated that in June 2013, the peteknyazev777@gmail.com account searched for the terms "kelihos" and "kelihos.f." *Id.* ¶ 55. Furthermore, the cellphone number provided by Google, ending in -0594, matched the phone number provided by Apple. *Id.*

Additionally, IP address analysis showed that peteknyazev777@gmail.com and Apple DSID 1972828024 shared temporal overlap with IP addresses, including IP address 91.122.62.16. *Id.* ¶ 50. IP address 91.122.62.16 was utilized by Defendant to purchase a digital certificate from the company GeoTrust. *Id.* ¶ 51.

Case 3:17-cv-00074-TMB Document 13-1 Filed 04/10/17 Page 12 of 35

Company records indicated that Peter LEVASHOV of Saint Petersburg, Russia initiated the purchase utilizing 91.122.62.16, and then completed the purchase minutes later with IP address 94.242.250.88. *Id.* As mentioned above, 94.242.250.88 is the IP address of the Kelihos server monitored by law enforcement, and which logged into pete777@mail.ru on thousands of occasions.

Furthermore, IP address 91.122.62.16 was also used by the Defendant to log into WebMoney account ending in 4986. *Id.* ¶ 68. WebMoney is an online payment system that allows for the use of multiple purses of different currencies. *Id.* In the course of the investigation, the FBI determined that WebMoney account -4986 contains a purse ending in -1018. *Id.* The FBI learned in the course of the investigation that purse -1018 was used by LEVASHOV to receive payment for his activities. *Id.* FBI analysis also indicated that the WebMoney account and Apple iTunes accounts were logged into via IP address 91.122.62.16 close in time to each other, indicating the Defendant as the single user utilizing both services. *Id.* ¶ 69.

Based on the above analysis connecting overlapping evidence from Kelihos servers, business records from Google, Apple and others, and financial accounts utilized by the operator of Kelihos, Defendant, Peter LEVASHOV, is the operator of Kelihos.

//

//

//

IV. KELIHOS HAS HARMED VICTIMS IN THIS DISTRICT AND THROUGHOUT THE UNITED STATES

By operating Kelihos, the Defendant has caused significant harm in this District and throughout the United States. Although it is impossible to fully quantify the losses the Defendant has caused, the paragraphs below provide the court with an overview of the scope of injury at issue.

Kelihos victims fall into two categories. First are the 1,250 to 10,000 victims in the United States whose computers are currently infected with Kelihos. *Id.* ¶ 8. These victims are subject to all of the harms discussed above, including having their computers coopted to distribute spam, their network traffic intercepted, their user credentials stolen, and their computer infected with other malicious programs. *Id.* ¶¶ 11-21.

The second group of victims are the recipients of the Defendant's fraudulent and malicious spam. As discussed above, these messages lure victims into fraudulent employment opportunities, attempt to infect their computers with malicious software, attempt to defraud them into purchasing worthless securities, and ply them with pharmaceuticals and other goods that appear legitimate but are actually counterfeit and potentially dangerous. *Id.* ¶¶ 12-18.

Representatives from both groups of victims are present in the District of Alaska. Numerous infected computers within the Kelihos botnet have IP addresses assigned by Alaskan ISPs, which is strong evidence that victims are located in Alaska. *Id.* ¶ 32. After identifying one such victim based in Anchorage, Alaska in

Case 3:17-cv-00074-TMB Document 13-1 Filed 04/10/17 Page 14 of 35

April 2016, the FBI contacted the victim, received consent to examine her computer, and was able to confirm that her computer was infected with Kelihos. *Id.* ¶¶ 32-33.

Persons in this District have also been the target of fraudulent and malicious spam emails that the Defendant has sent via the Kelihos botnet. *Id.* ¶¶ 34-35, 37, 39. These targets include employees of Alaska's public school districts, thousands of customers of Alaskan ISP General Communication Inc. (GCI), employees of the cities of Anchorage and Juneau, and employees of the Alaska Division of Occupational Licensing. *Id.* ¶¶ 34-35.

V. THE UNITED STATES IS PREPARED TO DISRUPT THE KELIHOS BOTNET

The FBI has developed a comprehensive technical plan to disrupt the Kelihos botnet. *Id.* ¶ 73. Successfully disrupting Kelihos requires a coordinated effort on the part of FBI and industry partners to sever the communication channels employed by the Defendant to control the infected computers within the botnet. *Id.* ¶ 73(e). The FBI will also attempt to remediate the Kelihos infection by identifying victims and contacting their internet service providers. *Id.* ¶ 73(f).

The Kelihos botnet is designed to operate by means of Peer to Peer (P2P) connectivity. *Id.* ¶ 73(a). A "peer" is another device infected by Kelihos. *Id.* ¶ 73(d). Instead of utilizing a centralized and readily identifiable Command and Control (C2) server to control all of the infected computers (peers), control is instead distributed across the entire infection base, which is intended to prevent law enforcement from easily targeting a readily identifiable C2 server and gaining

immediate control of the entire botnet. *Id.* ¶ 73(a). Computers infected with the Kelihos botnet, however, are designed to contact "Golden Parachute Domains" (redundant servers) if they cannot successfully connect peer to peer to distribute operating instructions. *Id.* ¶ 22.

Computers infected by Kelihos are divided into two groups: "router nodes" and "worker nodes." *Id.* ¶ 73(b). Router nodes communicate with both backend servers as well as other devices infected by Kelihos, and have publicly accessible IP addresses. *Id.* Router nodes are critical to the operation of Kelihos as they permit direct communication between the operator of the botnet and the infected computer, and comprise approximately 10% of the Kelihos botnet. *Id.*

In contrast, worker nodes comprise the remaining 90% of Kelihos infected devices, and utilize private IP addresses. *Id.* ¶ 73(c). Most devices accessing the internet do so by means of private IP addresses, as they are separated from the Internet by one or more intermediary networking devices such as a Wi-Fi router. *Id.*

For example, in many U.S. households, a Wi-Fi router is connected directly to a cable or DSL modem. *Id.* The Wi-Fi router is assigned the household's public IP address, while each device within the household accessing the wireless network is assigned a private, internal IP address. *Id.* Therefore, if a device accessing the internet through a Wi-Fi router or other networking device was infected, it would by contrast act as a "worker node" of the botnet. *Id.* Worker nodes using private IP

addresses, like a home computer connected to a Wi-Fi network, are more difficult for the botnet operator to maintain because they are not as readily accessible to the operator of the botnet as an infected device with a public IP address. *Id.*

To address the logistical challenge of maintaining contact with infected devices using private IP addresses (worker nodes), Kelihos commands its worker nodes to regularly check in with the router nodes. *Id.* ¶ 73(d). That automated "check in" process takes the form of exchanging so-called "peer lists," and "job messages." *Id.*

Peer lists consist of the IP addresses of other devices infected by Kelihos. *Id.* This information informs each infected device of the universe of other devices infected by Kelihos. *Id.* At a set interval, worker nodes will send a peer list and job request to a router node. *Id.* In response, the worker node then compares its own peer list with the received peer list, and updates its own peer list with new IP addresses until it reaches a maximum number of 3,000. *Id.* Router nodes also transfer job messages to worker nodes. *Id.*

To effectively combat the P2P structure of the Kelihos botnet, the FBI with assistance of private partners will participate in the exchange of peer lists and job messages with other infected computers. *Id.* ¶ 73(e). The FBI communications, however, will not contain any commands, nor will they contain IP addresses of any of the infected computers. *Id.* Instead, the FBI replies will contain the IP and routing information for the FBI's "sinkhole" server. *Id.* As this new routing

information permeates the botnet, the Kelihos infected computers will cease any current malicious activity and learn to communicate only with the sinkhole. *Id.* The effect of these actions will be to free individual infections from exchanging information with the Kelihos botnet and with LEVASHOV. *Id.* This will stop Kelihos's most immediate harm, the harvesting of personal data and credentials, and the transmittal of that data to servers under LEVASHOV's control. *Id.* Another portion of the Kelihos job messages is a list, known as the IP filter list. *Id.* This list functions as a type of blacklist, preventing communication with those IPs contained within the filter list. *Id.* If necessary, the FBI can also utilize this list to block Kelihos infected computers from continuing to communicate with router nodes. *Id.*

The sinkhole server will be a dead end destination designed specifically to neither decrypt nor capture content from the infected computers. *Id.* ¶ 73(f). The sinkhole server, however, will record the IP address and associated routing information of the infected machine so that the proper Internet Service Providers can be alerted of the existence of infected machines on their network and to monitor the effectiveness of the disruption effort. *Id.*

Additionally, because the Kelihos malware directs infected machines to request peer lists from the Golden Parachute Domains when they are unable to reach any peers, the disruption effort will not be effective unless those Golden Parachute Domains are also redirected to the sinkhole. *Id.* ¶ 73(g). In order to

prevent the defendant from using the Golden Parachute Domains to recapture peers, it is essential that these domains be kept out of the defendant's hands. *Id.* The Temporary Restraining Order sought as part of this action denies the defendant these domains through an order to the Domain Registries responsible for the U.S.-based top level domains requiring them to redirect connection attempts to the sinkhole server. *Id.*

VI. ARGUMENT

A. Jurisdiction and Venue Are Proper in This Court

Sections 1345 and 2521 of Title 18 authorize the United States to "commence a civil action in any Federal court" to enjoin fraud, and to "initiate a civil action in a district court of the United States" to enjoin illegal interception of communications. As detailed above, and in the Complaint filed herewith, Defendant is engaged in fraud and wiretapping against U.S. citizens and businesses on a massive scale. Accordingly, subject matter jurisdiction is proper in this Court. This Court may also exercise personal jurisdiction over Defendant, who is a foreign national that deliberately targeted victims in this District. Venue is proper under 28 U.S.C. § 1391(b)(2), for the reasons discussed below in relation to personal jurisdiction.

1. Defendant is Subject to Personal Jurisdiction in This Court Because He Has Defrauded and Engaged in Unauthorized Wiretapping of Victims in this District

At the complaint stage, a *prima facie* case by the plaintiff of personal jurisdiction is sufficient. *Boschetto v. Hansing*, 539 F.3d 1011, 1015 (9th Cir. 2008).

For claims arising under federal law, serving a summons or filing a waiver of service establishes personal jurisdiction over a defendant who is subject to the jurisdiction of a court of general jurisdiction in the state where the district court is located. Fed. R. Civ. P. 4(k)(1); *see Martinez v. Aero Caribbean*, 764 F.3d 1062, 1066 (9th Cir. 2014) ("Where, as here, there is no applicable federal statute governing personal jurisdiction, the district court applies the law of the state in which the district court sits." (internal quotation marks omitted)). Alaska's long-arm statute, AS § 09.05.015, allows for the exercise of personal jurisdiction "'to the maximum extent permitted by due process under the federal constitution.'" *Samson Tug and Barge Co., Inc. v. Koziol*, 869 F. Supp. 2d 1001, 1007 (D. Alaska 2012) (quoting *Glover v. Western Air Lines, Inc.*, 745 P.2d 1365, 1367 (Alaska 1987)). As such, "Alaska courts may exercise jurisdiction whenever the federal minimum contacts requirements are satisfied." *McCaffery v. Green*, 931 P2.d 407, 408 (Alaska 1997). This Court may assert personal jurisdiction if the defendant has sufficient "minimum contacts" with this forum such that subjecting the defendants to the court's jurisdiction comports with "traditional notions of fair play and substantial justice." *International Shoe Co. v. Washington*, 326 U.S. 310, 316-17 (1945). The Ninth Circuit has identified a three-part approach to evaluating personal jurisdiction. First, the defendant must purposefully direct his activities with the forum or resident thereof. Second, the claim must be one which relates to the defendant's forum-related activities. Finally, the exercise of jurisdiction must

comport with fair play and substantial justice, that is, it must be reasonable. *Insurance Co. of North America v. Marina Salina Cruz*, 649 F.2d 1266, 1267-70 (9th Cir. 1981). Where, as here, the cause of action is related to the defendant's contacts with the forum, it is sufficient if the contacts show "purposeful availment" by the defendant of an opportunity to conduct activity in the forum state. *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985) ("Jurisdiction is proper . . . where the contacts proximately result from actions by the defendant *himself* that create a "substantial connection" with the forum).

Here, Defendant's victims include many individuals and businesses within Alaska. Defendant has not only infected countless computers in Alaska with Kelihos, but has intentionally utilized domains specific to Alaska-based companies and government agencies to conduct further harm in Alaska and elsewhere. In so doing, Defendant has purposefully directed his conduct at Alaska. Moreover, the relief sought in this temporary restraining order relates directly to Defendant's activities, as it would wrest control of the very mechanism that has allowed Defendant to perpetrate his scheme. Finally, it is neither unfair nor inconsistent with "traditional notions of fair play and substantial justice" to subject Defendant to personal jurisdiction in this Court. Defendant has taken affirmative steps to spread the Kelihos botnet across the United States, and as a result, computers within Alaska have been infected with malicious code. Accordingly, Defendant's conduct

readily satisfies the "minimum contacts" requirement of due process, and personal jurisdiction is consistent with Alaska state law.

2. The Court Should Authorize Service of Process by In-Person Delivery, Delivery to Defendant's Last-Known Physical Address and Email Addresses, and Internet Publication

Unless otherwise prohibited by federal law or international agreement, an individual outside the United States may be served "as the court orders." Fed. R. Civ. Pro. 4(f)(3). The method of service selected must be "reasonably calculated, under all circumstances, to apprise interested parties of the pendency of the action" and afford them an opportunity to be heard." *Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950).

Here, the Government will serve the TRO and related filings ("Court Filings") on Defendant at the time of his apprehension, which is planned to coincide with the technical takedown measures. In the event that the Government cannot serve the Court Filings in person, the Government will effect service via certified mail to Defendant at the Spanish custodial facility. The government will also provide personal service upon any attorney representing Defendant in Spain and via publication on the Internet web sites of the Department of Justice or the FBI. If the TRO is granted, all press releases issued by the Department of Justice and the FBI with respect to this matter will direct Defendant and any potential co-conspirators to the websites where those pleadings can be accessed. There is therefore good cause to believe that even if the Government is unable to effect personal service,

Defendant will receive notice from any attorney representing Defendant in Spain, or he will seek additional information by visiting the public Internet sites of the Department of Justice and FBI and will thereby be notified of this action.

The Government is not aware of any international agreement that prohibits the methods of service proposed above. Accordingly, pursuant to Rule 4(f)(3), the Court should approve the Government's plan for service of process.

B. The Court May Authorize the United States to Implement the Technical Disruption Described Above to Stop the Ongoing Fraud and Unlawful Interception of Communications Perpetrated by the Kelihos Botnet

As described in more detail above, the TRO sought by the Government would: (1) distribute peer lists and job messages containing the IP and routing information for the FBI's sinkhole server; (2) distribute job messages containing an IP filter list preventing remediated computers from becoming infected again or conducting any further harm; and (3) direct Verisign and Afilias, both Internet Domain Registries, to block access to three domain names used to control Kelihos bots and to redirect connection requests to the server controlled by the Government. By ordering this relief, the Court will halt Defendant's use of the Kelihos botnet to defraud and wiretap U.S. citizens and businesses, and will preserve the status quo while private-sector partners identify and notify victims and assist in removing the Defendant's malicious software from their computers.

District courts generally have broad discretion in deciding whether to grant injunctive relief. *See Northwest Envtl. Def. Ctr. v. Bonneville Power Admin.*, 477

F.3d 668, 680 (9th Cir. 2007). This is particularly true "[w]here the public interest is involved," in which case "equitable powers assume an even broader and more flexible character than when only a private controversy is at stake." *Id.* (internal quotation marks omitted). In fact, as courts of equity, district courts "may, and frequently do, go much farther both to give and withhold relief in furtherance of the public interest than they are accustomed to go when only private interests are involved." *Virginian Ry. Co. v. System Fed'n No. 40*, 300 U.S. 515, 552 (1937).

The public interest in question has been formalized in Sections 1345 and 2521 of Title 18, which enhance the Court's traditional powers at equity by allowing the Court to promptly enjoin ongoing fraudulent or unauthorized interception upon a suit by the Government. These statutes confer broad authorization for courts to enter restraining orders "at any time," or to "take such other action, as is warranted to prevent a continuing and substantial injury." 18 U.S.C. §§ 1345(b), 2521. In particular, Section 1345

> authorizes broad injunctive relief . . . for any violation of chapter 63 [and is] a powerful weapon in the government's anti-fraud arsenal. In addition to authorizing injunctive relief . . . the statute empowers courts to enter restraining orders, prohibitions, and "take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of person for whose protection the action is brought." . . . As a result, civil suits under § 1345 are often used to preserve the status quo during a lengthy parallel criminal probe.

United States v. Payment Processing Ctr., 435 F. Supp. 2d 462, 464 (E.D. Pa. 2006) (quoting 18 U.S.C. § 1345(b)); *see also id.* at 466 (citing *United States v. Cen-Card*

Agency/C.C.A.C., No. 88-5764, 1989 WL 30653 (3d Cir. March 23, 1989) (discussing past use of Section 1345 to stop fraud)). Indeed, Congress enacted Section 1345 specifically "to allow the Attorney General to put a speedy end to a fraud scheme by seeking an injunction in federal District Court whenever he determines he has received sufficient evidence of a violation of Chapter 63 to initiate such an action," and intended the district court "to grant such action as is warranted to prevent a continuing and substantial injury to the class of persons designed to be protected by the criminal statute." S. Rep. No. 98-225, at 402 (1984). The use of similar statutory language in Section 2521, enacted after Section 1345, suggests a similar congressional intent to permit the Attorney General to "put a speedy end" to ongoing unlawful interceptions. *See also* S. Rep. No. 99-541, at 34 (1986). The Government seeks the relief set forth herein for precisely those purposes.

Civil injunctive relief, such as that sought in this application, has been used in several districts to accomplish large-scale disruptions of widespread computer hacking. In some cases, the United States Government has been the plaintiff, and in others, a private party has sought the injunctions. In all cases, injunctions have enabled the plaintiffs to halt hackers' schemes without infringing upon the privacy or property interests of victims or other parties.

For example, in Coreflood, the United States District Court for the District of Connecticut, pursuant to 18 U.S.C. §§ 1345 and 2521, enjoined a series of John Doe

defendants from running the Coreflood botnet software.[3] *United States v. John Doe et al.*, No. 3:11-CV-561 (D. Conn. April 11, 2011). The court based its ruling on the Government's showing that the John Doe defendants were using Coreflood to commit wire and bank fraud and to engage in unauthorized electronic surveillance, that the defendants' conduct was causing a continuing and substantial injury, and that the requested restraining order would prevent or ameliorate that injury. The Coreflood order authorized the FBI to establish a substitute server to replace the botnet command and control server formerly run by the defendants and compelled the Domain Registries and Registrars responsible for the domain names used by the Coreflood malware to redirect to the substitute server all traffic intended for the Coreflood domains.

More recently, the United States District Court for the Western District of Pennsylvania enjoined defendants from running the Dridex, Gameover Zeus (GOZ) and Cryptolocker malware also pursuant to 18 U.S.C. §§ 1345 and 2521. *See United States v. Ghinkul*, No. 2:2015-CV-1315 (W.D. Pa., filed October 8, 2015) ("Dridex");

---

[3] 18 U.S.C. § 1345, combined with the court's inherent equitable authority, was also the basis upon which the U.S. District Court for the Eastern District of Missouri entered a temporary restraining order enjoining individuals from transferring domain names and ordering registrars and registries not to change registration for specified domains, and subsequently entered a permanent injunction with the additional requirement that the registration of defendants' domain names be transferred to non-U.S. registrars. *United States v. Betonsports PLC*. No. 4:06CV01064, 2006 WL 3257797, at *8-9 (E.D. Mo. Nov. 9, 2006); Temporary Restraining Order, *United States v. Betonsports PLC*, No. 4:06CV01064 (E.D. Mo. July 17, 2006).

United States v. Bogachev, No. 2:14-CV-0685 (W.D. Pa. May 26, 2014). These orders, as was the case in Coreflood, authorized the FBI to establish a substitute server to replace the botnet command and control server formerly run by the defendants and compelled the Domain Registries and Registrars responsible for the domain names used by the malware to redirect to the substitute server all traffic intended for the criminal domains.

Similarly, in Microsoft's action against the ZeroAccess botnet, the Western District of Texas entered an injunction granting very similar relief to the relief sought here. *Microsoft Corp. v. John Does 1-8*, No. 1:13-CV-1014 (W.D. Tex. Nov. 25, 2013). Specifically, the court ordered Domain Registries to redirect traffic from ZeroAccess domains to a substitute command and control server, and ordered 45 U.S. ISPs to block their customers from connecting to a series of malicious IP addresses specified by Microsoft. Microsoft has obtained similar injunctions in a number of courts throughout the country, including a 2011 injunction for a prior version of the Kelihos Botnet. *See, e.g.*, *Microsoft Corp. v. John Does 1-5*, No. CV 15-6565 (E.D.N.Y. Nov. 23, 2015) (Dorkbot Botnet); *Microsoft Corp. v. John Does 1-3*, No. 1:15-cv-240 (E.D.V.A. Feb. 20, 2015) (Ramnit Botnet); *Microsoft Corp. v. John Does 1-8*, No. 1:14-cv-811 (E.D.V.A. June 27, 2014) (Shylock Botnet); *Microsoft Corp. v. John Does 1-82*, No. 3:13-cv-319 (W.D.N.C. May 29, 2013) (Citadel Botnet); *Microsoft Corp. v. Patti et al.*, No. 1:11-CV-01017 (E.D. Va. Sept. 22, 2011) (Kelihos Botnet); *Microsoft Corp. v. John Does 1-11*, No. 2:11-CV-00222 (W.D. Wash. Feb. 9,

2011) (Rustock Botnet); *Microsoft Corp. v. John Does 1-27*, No. 1:10-CV-156 (E.D. Va. Feb. 22, 2010) (Waledac Botnet).

1. Statutory Framework

Section 1345 of Title 18 authorizes the Attorney General to commence a civil action for injunctive relief whenever "a person is violating or about to violate this chapter." 18 U.S.C. § 1345(a)(1)(A). The referenced chapter of Title 18 includes Section 1343 (Fraud by wire, radio, or television), a statute the defendant is flagrantly violating through the use of the Kelihos botnet. Section 1345 further provides that a "permanent or temporary injunction or restraining order shall be granted," and that the "court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought." 18 U.S.C. §§ 1345(a)(3), (b).

Section 2521 of Title 18 similarly authorizes injunctions against illegal interception of communications in violation of 18 U.S.C. § 2511:

> Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the

United States or to any person or class of persons for whose protection the action is brought.

Because the Kelihos botnet harvests user credentials by illegally intercepting the communications between infected computers and Internet websites, Section 2521 also empowers the Government to seek the injunctive relief proposed in this action.

2. The United States May Obtain an Injunction Under 18 U.S.C. § 1345 and 18 U.S.C. § 2521 Without Demonstrating the Traditional Prerequisites for Injunctive Relief

Where, as here, the United States seeks an injunction pursuant to federal statutes enacted to protect the public interest that provide for injunctive relief, the Court is authorized to issue the injunction if the statutory conditions are satisfied and there is some cognizable danger of recurrent violation. *See United States v. Cole*, 84 F. Supp. 3d 1159, 1169 (D. Or. 2015); *United States v. Rhody Dairy, L.L.C.*, 812 F. Supp. 2d 1239, 1245-46 (W.D. Wash. 2011); *United States v. Moser*, 2005 WL 3277965, at *3 (D. Haw. Oct. 17, 2005). . The United States thus is not required to demonstrate the traditional prerequisites for a TRO or preliminary injunction, such as irreparable harm or sufficient public interest. *United States v. Estate Pres. Servs.*, 202 F.3d 1093, 1098 (9th Cir. 2000) ("The traditional requirements for equitable relief need not be satisfied since [the statute] expressly authorizes the issuance of an injunction."); *United States v. Odessa Union Warehouse Co-Op*, 833 F.2d 172 (9th Cir. 1987) ("Where an injunction is authorized by statute, and the statutory conditions are satisfied as in the facts presented here, the agency to whom the enforcement of the right has been entrusted is not required to show irreparable

injury."). *See also United States Postal Service v. Beamish*, 466 F.2d 804, 806 (3d Cir. 1972); *CSX Transp., Inc. v. Tennessee Bd. Of Equalization*, 964 F.2d 548, 551 (6th Cir. 1992); *Government of the Virgin Islands v. Virgin Islands Paving*, 714 F.2d 283, 286 (3d Cir. 1983) (superseded on other grounds by statute, *see Edwards v. Hovensa*, 497 F.3d 355, 359 (3d Cir. 2007); *United States v. Hayes Int'l Corp.*, 415 F.2d 1038, 1045 (5th Cir.1969); *United States v. Livdahl*, 356 F. Supp. 2d 1289, 1290-91 (S.D. Fla. 2005); *United States v. Sene X Eleemosynary Corp.*, 479 F. Supp. 970, 980–81 (S.D. Fla. 1979) ("It is sufficient to show only that the threatened act is within the declared prohibition of Congress."); *United States v. Nutrition Serv., Inc.*, 227 F. Supp. 375, 388–89 (W.D. Pa. 1964, *aff'd* 347 F.2d 233 (3d Cir. 1965).[4]

3. The United States Is Authorized to Obtain Injunctive Relief Under 18 U.S.C. § 1345 and 18 U.S.C. § 2521 Because Defendant Is Committing Wire Fraud and Illegally Intercepting Electronic Communications

As detailed in Special Agent Peterson's Declaration, and summarized above, Defendant is engaged in wire fraud and illegal interception of communications on a massive scale through the use of Kelihos. The United States is therefore fully authorized to obtain an injunction under both 18 U.S.C. § 1345 and 18 U.S.C. § 2521.

When, as here, a federal statute empowers the Government to obtain an injunction prohibiting further violations of criminal law, courts are split on whether

[4] In passing a statute authorizing injunctive relief, Congress implicitly finds that a violation of the law will irreparably harm the public interest. *See United States v. Cole*, 2014 WL 1303143, at *3 (D. Or. Mar. 31, 2014).

the United States must show that there is probable cause to believe the defendant is violating or is about to violate any of the enumerated offenses, or must demonstrate such violations by a preponderance of the evidence. *Compare United States v. Luis*, 966 F.Supp.2d 1321, 1326 (S.D. Fla. 2013) (probable cause; collecting cases) and *United States v. Payment Processing Ctr., LLC*, 461 F. Supp. 2d 319, 323 & n.4 (E.D. Pa. 2006) (probable cause) with *United States v. Brown*, 988 F.2d 658, 663 (6th Cir. 1993) (preponderance) and *United States v. Williams*, 476 F.Supp.2d 1368, 1374 (M.D.Fla.2007) (preponderance). This issue has not been decided by the Ninth Circuit. In any event, given the overwhelming evidence of criminal conduct presented in Special Agent Peterson's Declaration, the United States easily meets its burden of proof under 18 U.S.C. § 1345 and 18 U.S.C. § 2521 regardless of which evidentiary standard is applied.

a. Defendant is Committing Wire Fraud (18 U.S.C. § 1343)

The elements of wire fraud are: (1) a scheme to defraud; (2) use of the wires for the purpose of executing the scheme; and (3) fraudulent intent. *United States v. Jinian*, 725 F.3d 954, 960 (9th Cir. 2013). Defendant's conduct readily establishes all of these elements. Defendant operates the Kelihos botnet for the purpose of stealing online credentials and using those credentials to gain unauthorized access to email accounts and web services. Once these credentials are harvested, they are used by Defendant or others to compromise the relevant accounts. For example, email logins and passwords are compromised to further Defendant's high volume

distribution of spam. Moreover, the nature of the spam is often designed to defraud its recipients. Common spam campaigns include schemes to sell counterfeit or grey market prescription drugs as authentic, mislead individuals to apply for fictitious work-from-home jobs which are nothing more than vehicles to launder money or steal the individual's money, or pump and dump security schemes, which trick individuals into purchasing securities with the promises of unlikely gains, all so that cybercriminals can profit off artificially inflated stock gains.

b. Defendant is Unlawfully Intercepting Electronic Communications (18 U.S.C. § 2511)

It is a violation of the Wiretap Act to:

> intentionally intercept, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> [or to]
>
> intentionally use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.

18 U.S.C. §§ 2511(1)(a), (d); (4)(a). As described in the Declaration of Special Agent Peterson, Kelihos is a highly advanced communications interception platform that exists, in part, to harvest online credentials by intercepting communications of the infected computer. Through the use of Kelihos, these credentials are harvested in real time as they are transmitted from the victim's computer. This conduct clearly violates 18 U.S.C. §§ 2511(1)(a) and (d).

c. The Violations Caused by the Kelihos Botnet are Ongoing and Recurring

There is a strong likelihood of recurrent violation because the crimes committed through the Kelihos botnet are ongoing. The continued proliferation of the Kelihos botnet despite prior takedown efforts by the private sector is evidence of the botnet's aggressive and prolonged nature. *See Patti et al.*, No. 1:11-CV-01017 (E.D. Va. Sept. 22, 2011). Even without the Defendant at the helm, the Kelihos botnet could easily fall into the hands of another criminal and could be used to infect other computers, harvest credentials and financial information, and intercept communications, all in violation of U.S. law.

4. *Ex Parte* Relief is Appropriate

The purpose of a temporary restraining order is to preserve the status quo until the Court has an opportunity to pass on the merits of a preliminary injunction. *See Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers Local No. 70*, 415 U.S. 423, 439 (1974); *Garcia v. Yonkers Sch. Dist.*, 561 F.3d 97, 107 (2d Cir. 2009). A district court may grant a temporary restraining order without notice to defendants if "specific facts in an affidavit or verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition," and the movant "certifies in writing any efforts made to give notice and the reasons why it should not be required." Fed. R. Civ. P. 65(b)(1).

The relief sought herein would preserve the status quo by preventing Defendant from defrauding additional individuals. As discussed herein, the ongoing and aggressive fraud the Government seeks to stop will continue to cause irreparable injury and loss until it is halted. Prior notice to Defendant would render futile the Government's efforts to stop his ongoing criminal acts. If notified in advance of the Government's intended actions, Defendant or his agents could change his malware, shift the domains, change IP addresses, or take other technical steps – which would not require substantial time or effort – to avoid the planned disruption of his operations. *See* Peterson Declaration ¶ 71. The requested *ex parte* relief is necessary to prevent such evasion of the Government's remedial measures. *See* 18 U.S.C. §§ 1345(b) (the "court shall . . . take such other action as is warranted to prevent a continuing and substantial injury"), 2521 (same); Fed. R. Civ. P. 65(b)(1).

5. A Sealing Order Should be Entered in this Case

As set forth in the Government's request for leave to file under seal, the Government respectfully requests leave to file this memorandum, the proposed TRO and all associated documents under seal.

//

//

//

//

Conclusion

For the foregoing reasons, the Government respectfully requests the Court grant the Temporary Restraining Order requested by the Government.

RESPECTFULLY SUBMITTED, on April 4, 2017 at Anchorage, Alaska.

BRYAN SCHRODER
Acting United States Attorney

By: /s/ Richard Pomeroy
RICHARD POMEROY
YVONNE LAMOUREUX
ADAM ALEXANDER
Assistant U.S. Attorneys
District of Alaska

KENNETH A. BLANCO
Acting Assistant Attorney General

By: /s/ Ethan Arenson
ETHAN ARENSON
HAROLD CHUN
FRANK LIN
Trial Attorneys
Computer Crime and
Intellectual Property Section